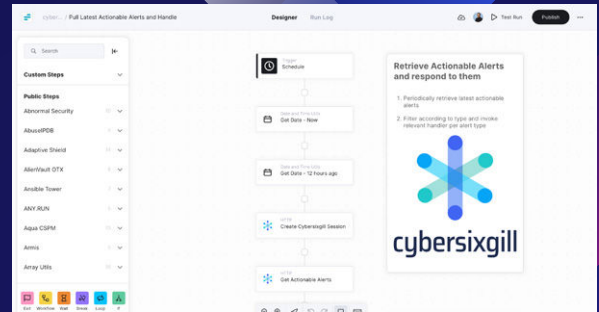




INTELLIGENCE-DRIVEN SECURITY AUTOMATION FOR END-TO-END THREAT PROTECTION



The Intelligence-Action Deficit

Security teams are well aware of the vital roles that security automation and threat intelligence solutions play within the modern security stack. Unfortunately, these two core cybersecurity functions are often disconnected, creating a deficit between intelligence and action.

This means threat detection (intelligence) and threat response (action) are siloed and out of sync, resulting in high-risk exposures and a staggering average mean time to detect and respond (MTTR+D) of 287 days.

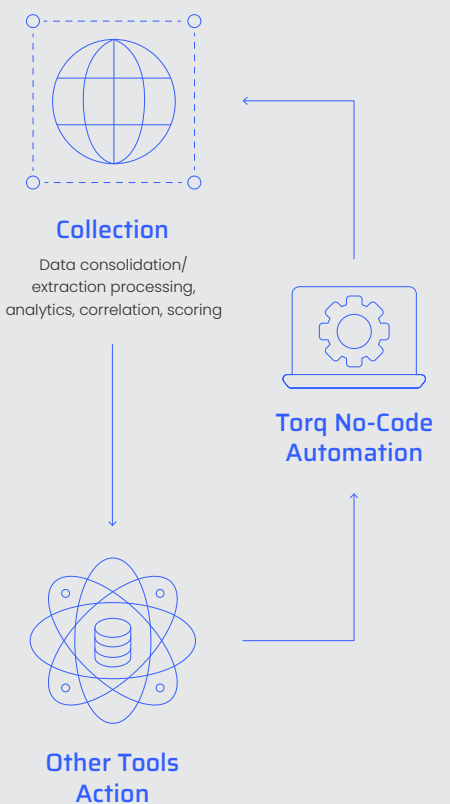
Threat context and prioritization are critical prerequisites for automated response. By integrating relevant, prioritized, context-rich threat intelligence with orchestrated/automated processes, teams unlock the full potential of existing security stacks—saving time and resources while streamlining response and remediation.

Cybersixgill & Torq: End-to-End No Intervention Threat Protection

Cybersixgill has partnered with Torq to bridge the divide between intelligence and action, operationalizing Cybersixgill's market-leading threat intelligence through seamless no-code security automation in Torq. With this strategic partnership, Cybersixgill and Torq pioneer end-to-end, no-intervention threat protection, dramatically reducing MTTR+D through customizable automated workflows, triggered by actionable, context-rich threat intelligence from the cybercriminal underground.

“ Torq and Cybersixgill make it easy for teams to turn manual security processes into automated, intelligence-driven workflows within minutes, eliminating reactive processes to build a resilient, proactive cybersecurity posture. ”

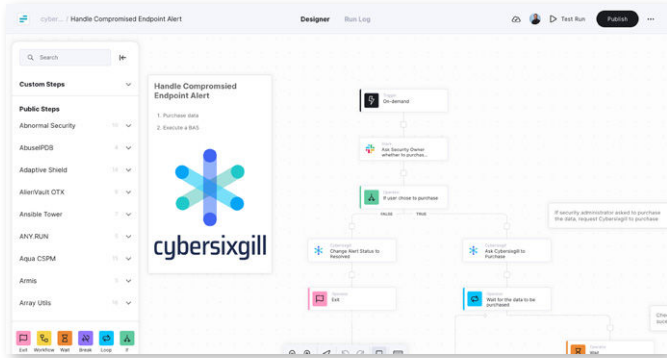
Cybersixgill Threat Intelligence





Features:

- Easily integrate Cybersixgill's threat intel into your tech stack to automate custom response workflows – without writing a single line of code.
- Automatically respond or remediate issues the instant Cybersixgill detects potential risks.
- Harness rich threat context from Cybersixgill in automated threat hunting workflows, instantly enriching event data from other tools.



Cybersixgill + Torq Benefits

- **Reduce Risk** with automated, end-to-end intelligence-driven remediation and response workflows. Block threats as they emerge, accelerating MTTR+D.
- **Save Time** and eliminate redundant tasks, tools, and processes with no-code workflows that can be built and deployed in hours, offering near-immediate time to value.
- **Minimize Cost** and optimize efficiency by automating processes with a consolidated threat protection solution, maximizing value from existing security investments.

About Cybersixgill

Cybersixgill continuously collects and exposes the earliest possible indications of risk moments after they surface on the clear, deep and dark web.

Our extensive body of threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer pain points and use cases. These solutions are scalable, searchable and seamlessly integrated into existing security stacks, arming teams with critical insights to proactively block threats before they materialize into attacks.

For more information, visit cybersixgill.com and for more details: info@cybersixgill.com.

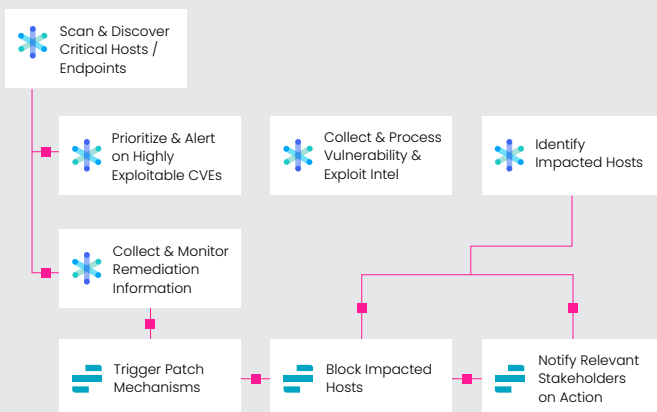
About Torq

Torq is a no-code automation platform for security teams. Torq's limitless connectivity, intelligent automation, and curated templates help security professionals accelerate threat response and remediation, identify and mitigate risks, and deliver protection at the speed of modern business. Founded in 2020, the company is backed by Insight Partners, SentinelOne, GGV Capital and Bessemer Venture Partners. Torq has offices in Portland, Oregon, New York City, and Tel Aviv, Israel.

For more information, visit torq.io.

Use Case Examples

Vulnerability Management & Prioritization



Compromised Access to Organization

